

Table of Contents

A 1

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

- **Access**: The act of accessing a particular zone or particular assets.
- **Access control**: The act of restricting unauthorized people from accessing the infrastructure and assets. Access made by authorized individuals is recorded in the [log](#).
- **Access Group**: A [user group](#) that has the right to access a specified [door/door group](#) during a scheduled period of time.
- **Access Level**: The right to access the [door](#) during a scheduled period of time.
- **Access on Card**: A card on which information about a user's ID, [credential](#), and [access group](#) is recorded.
- **Access Rule**: A rule concerning access to a certain [door/door group](#) during a scheduled period of time.
- **ACID**: The ACID represents four main properties that a transaction should have, the terminology stands for Atomicity, Consistency, Isolation and Durability. Atomicity, as the very basic operation unit, requires each transaction to be 'all or nothing', or simply all-success or all-fail. Consistency ensures any transaction to bring the database from one valid state to another. Isolation ensures the [transaction](#) in process must remain isolated from any other transactions. Durability ensures integrity that committed data is kept in the drive even in the event of failure for restructure.
- **Ad Hoc Network**: A network that is autonomously configured by each device without reliance on network infrastructure such as a base station and an access point. In this network, a dynamic and autonomous network topology is formed despite each device communicating through a wireless interface, as each device can be moved freely thanks to a routing function that enables the distance limitations of wireless communication to be overcome.
- **Administrator**: The user who has full access to the configuration software.
- **AES (Advanced Encryption Standard)**: The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST).
- **Alarm**: Among events occurred in the system, the type of [event](#) that requires action without delay.
- **Alarm action**: The actions that automatically perform activities such as controlling the device and sending emails when an alarm or a certain event occurs.
- **Alert**: The act of displaying or forwarding in real time an [alarm](#) event occurred in the system.
- **Analog intercom**: An intercom telephone that consists of an analog switch and a network.
- **ANSI 378**: The fingerprint template standards defined by the American National Standards Institute

(ANSI).

- **AP (Access Point)**: A device for implementing a **Wireless LAN**. An access point creates a connection to a wireless network through a wired LAN.
- **APB (Anti-passback)**: A structural method used to control access. This function uses access control devices installed both inside and outside the door, so that authentication is required for access to the zone. In the case of card-based access control systems, if a person enters a zone following the person in front without swiping their card on the reader, the door does not open when the person attempts to leave the zone, and subsequently an anti-passback event occurs. Anti-passback is categorized into hard APB and soft APB. If the anti-passback is violated, the anti-passback event is created immediately and hard APB does not permit access to the user while soft APB still permits access to the user.
- **API (Application Programming Interface)**: An API is a set of protocols, tools, and instruction for implementing software applications. In case of web application development, the API specifies how the system should send requests and what kind of corresponding responses should be expected to receive. The API may include functions like file managements, window/video/character processing to ease the application development process for the 3rd party application developers.
- **Arm**: The act of monitoring a specific zone for the prevention of crime and accidents. 24-hour monitoring, alarm notifications, recordings, etc. are available through a security system.
- **Audit trail**: The data recorded on system changes. The audit trail makes it possible to search for information about unauthorized user activity, the processing of user activity, etc.
- **Authentication**: The act of verifying the **credentials** entered by a user to identify the user.
- **Authentication mode**: A combination of **credentials** required for **authentication**.

From:

<http://kb.supremainc.com/knowledge/> -

Permanent link:

http://kb.supremainc.com/knowledge/doku.php?id=en:e_a

Last update: **2019/01/09 10:21**